19772 Pauling • Foothill Ranch, CA 92610-2611 USA
TEL: (949) 465-3000 • FAX: (949) 465-3020
www.imcnetworks.com

Document Number 56-80303-00 A2
June 2000

ROUTERSCREEN™

installation guide

© 2000 IMC Networks. All rights reserved.

The information in this document is subject to change without notice. IMC Networks assumes no responsibility for any errors that may appear in this document. **RouterScreen** is a trademark of IMC Networks. Other brands or product names may be trademarks and are the property of their respective companies.

About RouterScreen

RouterScreen™ from IMC Networks is a 10 Mbps Ethernet modular networking device that provides packet filtering and bandwidth control to increase performance of an attached router and maximize use of the LAN/WAN connections.

RouterScreen is available as a standalone, plug-and-play unit, or as a module for installation in an IMC Networks **PowerChassis/101™**.

RouterScreen features two RJ-45 data ports (labeled LAN and WAN), as well as a separate RJ-45 port designated by default for SNMP management traffic (i.e., the management port). It also features a DB-9 serial port for performing initial IP information configuration (see page 5 for more information on using this port).

Although *RouterScreen* provides a twisted pair port solely for management traffic, you can configure *RouterScreen* to accept SNMP management traffic from any of its three ports. All three ports may also be configured for Half-Duplex (HDX) or Full-Duplex (FDX) operation (set this based on the capabilities of the connected hardware).

QUICK START

Dip Switch Configuration 1
Installation Instructions 2
Initial Set-Up 4
About iView 7
Configuring RouterScreen 8
Packet Filtering Modes 9
Bandwidth Control 11
LEDs 12
Troubleshooting 13

Dip Switch Configuration

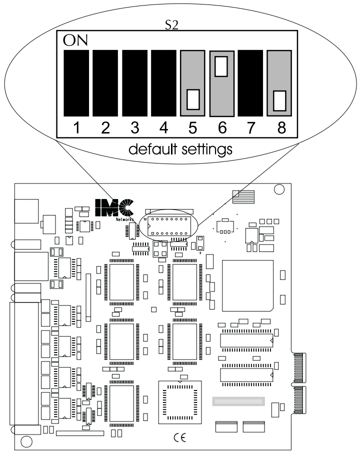
Before installing a modular *RouterScreen* or connecting a standalone *RouterScreen* to your network, you may want to change the module/unit's default Dip switch settings.

RouterScreen's Dip switches control the Duplex mode of the port labeled "Mgmt." (default is Half-Duplex) as well as designate one of *RouterScreen*'s three ports for management traffic (default is "Mgmt." port).

See the following graphic for the Dip switch location and settings.

NOTE

The Duplex mode of the data ports (LAN and WAN) is set via the management software.



S2
Dip switches **5** and **6** set port for SNMP management traffic

Switch 5	Switch 6	Result
Off	Off	No SNMP
Off	On	SNMP on Mgmt. Port
On	Off	SNMP on LAN Port
On	On	SNMP on WAN Port

Dip switch **8** sets management port's Duplex Mode
On = FDX OFF = HDX (DEFAULT)

Dip switches **1-4**, **7** are Factory Configured
(**DO NOT CHANGE**)

Figure 1: *Dip Switch Location and Settings*

ACCESSING DIP SWITCHES ON PRE-INSTALLED MODULES

If your *RouterScreen Module* shipped from the factory pre-installed in an IMC chassis, you will need to loosen the captive screws and gently slide the module out of the chassis to access the Dip switches. See the installation instructions on page 3 to re-install the module when finished.

ACCESSING DIP SWITCHES ON STANDALONE UNITS

In order to access the Dip switches on a standalone (non-modular) *RouterScreen*, you will need to remove the unit's cover. Follow these instructions:

1) Turn OFF any power to the unit, and UNPLUG THE POWER CORD!

2) Remove the rackmount ears, if attached.

3) Using a Phillips screwdriver, remove the six screws on top and four screws on each side of the cover.

4) Remove the cover (see graphic, right). Set the Dip switches as desired.

5) Replace the cover, making sure the top screw holes found on each side of the cover are in the front. Replace and tighten the screws to secure the cover.

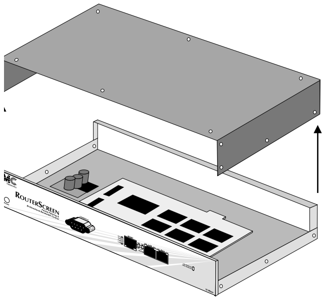


Figure 2: *Removing the cover of a non-modular RouterScreen to access the unit's Dip switches.*

Installing RouterScreen

Once the Dip switches are set, you are ready to install your *RouterScreen* module/unit. For instructions on installing a module into a chassis, see the instructions directly below. If you have a standalone unit, skip ahead to the tabletop or rackmount installation instructions that follow.

MODULE INSTALLATION

To install a *RouterScreen Module*, slide the module into the chassis, via the cardguides, until the module is seated securely in the connector. Secure the module to the chassis by tightening the captive screws. Once the module is installed, you will need to connect the chassis to your network. See the tabletop or rackmount installation instructions below for directions.

> **NOTE**
>
> *RouterScreen* modules may be installed when the power is on — i.e. they are "hot-swappable."

TABLETOP INSTALLATION INSTRUCTIONS

To connect any *RouterScreen* to your network, first place the chassis/unit on a suitable flat surface, leaving some space at the back of the unit to accommodate cooling. Use CAT-3 or better cables to attach *RouterScreen* to the router using the WAN port, the local area network using the LAN port, and (optionally, depending on Dip switch configuration) the management network using the management port. Plug *RouterScreen* into a reliable, filtered power source.

RACKMOUNT INSTALLATION INSTRUCTIONS

For a rackmount installation, you will need four #10 screws and four clip nuts (hardware may vary by rack type). The rest of the hardware is supplied with the unit.

First, mount the RETMA mounting ears to the chassis/unit by removing the screws on each side of the front edge of the unit. Use these screws to attach the supplied mounting ears. Next, locate a suitable location on the rack for installation. Secure the clip nuts on to the mounting rails, and use the #10 screws to attach the chassis/unit to the rack. Finally, using CAT-3 or better cables, attach *RouterScreen* to the router using the WAN port, the local area network using the LAN port and (optionally, depending on Dip switch configuration) the management network using the management port. Plug *RouterScreen* into a reliable, filtered power source.

When installing a chassis/unit in an equipment rack, be sure to observe the following precautions to prevent electrical or mechanical damage:

- Stay within the chassis'/unit's power rating to prevent overload of supply circuits or damage to overcurrent protection and supply wiring.
- Maintain reliable earth ground, especially when connecting to power strip instead of directly to branch circuit.
- Protect your chassis/unit from exposure to sunlight and electrical or magnetic fields.

- Ensure that the equipment rack remains stable, even with the addition of the chassis/unit and its associated cabling.

Configuration Steps

Once connected to your network, you must perform the following steps to configure your *RouterScreen* module/unit.

- Assign IP information to *RouterScreen* using either HUBCTRL32 or the unit's serial port so that it is accessible via SNMP.
- Install **iView™ for RouterScreen** or another SNMP-based management application onto the management PC.
- Set the data port's bandwidth control settings, Duplex modes and packet filtering modes using *iView* or other SNMP application.

About Initial Set-Up

In order to configure and manage *RouterScreen*, it is first necessary to give it an IP address so that it is accessible via SNMP. There are two ways to assign this IP information to *RouterScreen*:

- using HUBCTRL32™ (requires Windows 98/NT/2000™)
- via the unit's serial port

Besides assigning an IP address and subnet mask, both methods will also allow you to create community strings, assign access rights, send traps and more. However, HUBCTRL32 offers more options than the serial port method (e.g., you can select *which* traps to assign with HUBCTRL32).

USING HUBCTRL32

HUBCTRL32 (HubControl 32) is an in-band configuration utility created by IMC Networks that lets users quickly and easily complete the first stages of SNMP configuration for IMC Networks SNMP-manageable devices. Tasks HUBCTRL32 can perform include:

- setting the IP address, subnet mask and default gateway;
- defining the community strings and SNMP traps; and
- setting PPP parameters for remote management.

In addition to the above functions, HUBCTRL32 offers an authorized IP address system and access restriction to MIB groups supported by IMC Networks manageable devices. These extra layers of security are purely optional and do not effect SNMP compatibility in any way.

HUBCTRL32 can also be used to upload new versions of the system software and new MIB information. It also offers diagnostic capabilities for faster resolution of technical support issues.

HUBCTRL32 works with the following platforms:

- Windows NT 4.x
- Windows 98
- Windows 2000

HUBCTRL32 can be found on the *iView* CD, or you can download it from the IMC Networks Web site at the following URL: **www.imcnetworks.com/tech/software.htm**.

NOTE

HUBCTRL is also available in a DOS version. Please contact IMC Networks technical support at support@imcnetworks.com for more information.

For information regarding the installation and use of HUBCTRL32, refer to the HUBCTRL32 installation guide or the HUBCTRL32 online help file.

USING SERIAL PORT TO ASSIGN IP INFORMATION

Following are instructions for using the unit's serial port to assign IP information to *RouterScreen*. Note that this is the IP address used by SNMP to address *RouterScreen* itself, NOT an IP address associated with non-management traffic screened by the LAN or WAN ports.

Connecting RouterScreen

RouterScreen's serial port uses an IBM-compatible DB-9 serial connector. To connect the device to your terminal/computer, use the enclosed DB-9 cable. (If your computer/terminal has a serial port using a connection not compatible with a DB-9 COM port, use the Pin Connection table below for reference in making a cable.) Plug one end of the cable into the DB-9 connector on the device, and the other into the appropriate port on your computer/terminal. Set your computer/terminal for VT-100 emulation. The serial port on the computer/terminal should be set for **38.4K BAUD, 8 data bits, 1 stop bit, no parity, no flow control.**

DB-9 Pin Connection Chart

Pin #	Function
2	Transmit (OUT)
3	Receive (IN)
5	Ground
1,4, 6-9	Not used

Main Configuration Screen

After running through an initial self test, the screen will display the following message: "Press <Enter> for Device Configuration." Press **Enter** to be taken to the main configuration screen. Here you will find several displays:

Saved Values — displays changes made during current session.

- IP Address (*MUST be assigned during initial configuration*)
- Subnet Mask (*MUST be assigned during initial configuration*)
- Default Gateway

Current Values — displays values currently in use.

- IP Address (*IP address of SNMP agent*)
- Subnet Mask (*mask to define IP subnet agent is connected to*)
- Default Gateway (*default router for IP traffic outside subnet*)

Command List

- **I** = Enter New Saved Parameter Values
- **P** = Change Password
- **T** = New Trap Destination
- **K** = Remove ALL Trap Destinations
- **C** = New Community String
- **U** = Delete ALL Community Strings
- **E** = End Session

NOTE

You must reboot after making any modifications to the Saved Values or your changes will not take effect. To reboot, type the word "**Reboot**" (no quote marks) at the prompt on the main configuration screen, or turn the device's power OFF then ON again.

NOTE

Because the Delete key does not work on VT-100 terminal emulators, use the **F2** key instead.

Assigning IP Information

To modify the Saved Parameter Values (i.e., assign IP address and subnet mask), press **I**. You will be instructed to enter the IP address and subnet mask for the connected device. Press **Enter** after each. You may also assign a default gateway, if desired (press **Enter** to skip). When finished, press **Enter**, then type "**Reboot**" for changes to take effect. The Saved Values and Current Values should now both display the changes made (e.g., new IP address and subnet mask).

Creating/Deleting Community Strings

The default community string is named "public" and has read/write access. For security reasons, IMC Networks recommends you set up two communities: one with read-only access (for general use), the other with read/write access (for the administrator).

To create a new community string, go to the main configuration screen and press **C**. Enter the name of the new community (up to 16 characters, no spaces allowed) and press **Enter**. Then type one of the following options to assign the community string's access rights:

- **R** = read-only access • **W** = read/write access • **Enter** = abort

Press **Enter**.

To delete all community strings and start over, press **U**. You will then be asked, "Are you sure you want to delete all future strings?" Press **Y** to proceed, **N** to abort. Press **Enter**. Note that the above function will delete ALL community strings. If you want to be able to selectively delete community strings, use HUBCTRL32 to configure your device.

Assigning/Removing Trap Destinations

Traps are sent by the manageable device to a management PC when a certain event takes place. To enter a trap destination, press **T**. You will then be asked to "Enter a New IP Address." Type the IP address of the destination device and press **Enter**. Then type the name of the community string (created earlier) and press **Enter**. All traps the device is capable of will be enabled. To remove ALL trap destinations, press **K**. You will then be asked if you really want to remove all trap destinations. Press **Y** to continue. Press **N** to abort. Press **Enter**.

Password Protection

You can password protect the serial configuration process by pressing **P** from the main configuration screen. You will be asked to enter a password. (***NOTE:*** *Passwords are case sensitive*.) Enter your password (spaces are NOT allowed) and press **Enter**. You will then be asked for your password whenever you log on or off. To remove password protection, select **P** and instead of entering a password, press **Enter**. Should you forget the password, use HUBCTRL32 to access the back-up copy of the PROM, then reburn the flash PROM (or contact IMC Networks technical support for assistance).

Ending Your Session

Be sure to press **E** before disconnecting the cable in order to stop the device from outputting to the serial port.

About iView

Once *RouterScreen* is assigned an IP address, you can use *iView* or another SNMP-based NMS application to configure and remotely manage *RouterScreen*.

iView is a cross-platform network management application for IMC Networks intelligent networking devices. It gives network managers the ability to monitor and control IMC Networks' products from virtually any 32-bit Windows platform. *iView* can also function as a snap-in module for many SNMP applications. Please consult the *iView* installation guide or *iView* CD for assistance in installing and launching *iView*.

Configuring RouterScreen

RouterScreen uses bandwidth control features in combination with packet filtering to streamline traffic that reaches the attached router and eventually the WAN connection.

Following is an example of a typical installation and related configuration instructions, followed by in-depth explanation of *RouterScreen*'s packet filtering, bandwidth control and other capabilities.

In the following example, a company installs *RouterScreen* between its LAN and router. (***NOTE***: *Router could be another Layer 3 device*.)

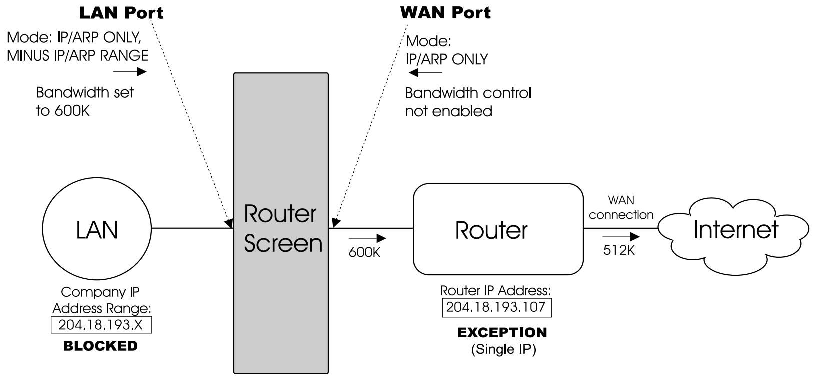


Figure 3: *Example of a Typical RouterScreen Installation*

Because the WAN connection operates at a speed of 512K, the company sets *RouterScreen*'s bandwidth in that direction to 600K — a little above the capacity of the WAN line. This helps create smoother traffic output to the WAN and distributes the buffer memory chores between both *RouterScreen* and the router.

To make sure the router's time (and buffer memory) isn't taken up sorting out traffic not intended to reach the WAN anyway, the company configures *RouterScreen* to handle the packet filtering in that direction. Using *RouterScreen*'s packet filtering modes (see next page), they set up a range of IP/ARP addresses for *RouterScreen* to block in that direction. The mode and range used (see table, next page) tells *RouterScreen* to discard packets addressed to devices within the company's IP address range, thereby keeping the LAN's internal traffic from reaching the router.

However, this range will also block traffic intended for the router itself (e.g., management traffic), since its IP address falls within the blocked IP address range. To solve this, the company uses *RouterScreen*'s **Single IP** function (see page 10), which allows one IP address to be excluded from the rule set up by the packet filtering mode. By entering the router's IP address as the Single IP, *RouterScreen* will allow packets addressed to the router to pass, even though they fall within the range of addresses it is told to discard.

As for traffic coming from the WAN/Internet into the LAN, the company sets *RouterScreen* to allow all IP/ARP traffic to pass, blocking only those protocols not recognized by the LAN.

EXAMPLE INSTALLATION SETTINGS

UNIT SETTINGS

Bandwidth Granularity: 1,000

WAN PORT

BPS Setting: 0 (not enabled)
Mode: IP/ARP ONLY*

LAN PORT

BPS Setting: 600
Mode: IP/ARP ONLY MINUS IP/ARP RANGE
Base IP: 204.18.193.0
Multiplexing Byte: D
Low Range: 1
High Range: 254
Single IP: 204.18.193.107

**Base IP, Multiplexing Byte, Range and Single IP functions are not applicable in IP/ARP ONLY mode used by the WAN port.*

ABOUT PACKET FILTERING

RouterScreen provides six modes for forwarding/discarding frames that come in contact with the device. These packet filtering modes should be configured individually for each data port (LAN and WAN).

The first two modes, All Protocols (default) and IP/ARP Only, allow all or almost all network traffic to pass through *RouterScreen*. These modes are used most often for traffic coming from the WAN or Internet, through the router and *RouterScreen*, and on to the LAN. The other four modes use specific IP address ranges, defined by the user, to tell *RouterScreen* to either pass on or discard traffic based upon its destination IP. These modes are either inclusionary or exclusionary, and are most often used to restrict traffic coming from LAN, through *RouterScreen*, and on to the router/Layer 3 device.

The six modes are as follows:

General Modes:

- **All Protocols** — Forwards ALL traffic. Can use this mode as a generic mode for incoming traffic to be forwarded on to the LAN.
- **IP/ARP Only** — Forwards all IP/ARP traffic; blocks all other protocols. Because this mode allows all IP/ARP traffic to pass through, this is the recommended mode for traffic coming from the Internet to the LAN in the example shown on opposite page (configured on WAN port).

Inclusionary Modes:

- **Non-IP/ARP, Plus IP/ARP Range** — Allows all non-IP traffic to pass; forwards only IP/ARP packets that fall into a specified range, discarding all other IP/ARP traffic.

- **IP/ARP Range Only** — Like previous mode, but blocks all non-IP traffic as well.

Exclusionary Modes:

- **All Protocols, Minus IP/ARP Range** — Forwards everything except what is specified in IP address range, including non-IP traffic.
- **IP/ARP Only, Minus IP/ARP Range** — Forwards all IP/ARP packets except what is specified in IP address range; discards non-IP traffic. Because this is the most efficient mode for blocking unnecessary traffic from reaching the router (unless using a non-IP protocol), this is the recommended mode for traffic coming from the LAN to the WAN/Internet in the example shown on page 8 (configured on LAN port).

Set the packet filtering mode based on the FIRST *RouterScreen* port (LAN or WAN) the traffic will come in contact with.

ADDITIONAL CONFIGURATION FOR PACKET FILTERING MODES

When using an inclusionary or exclusionary mode, you will also need to enter values for the following:

Required (*all inclusionary/exclusionary modes*):

- **Base IP** — A four-byte address that tells *RouterScreen* the common portion of the IP addresses for whose packets should be discarded (excluded) or forwarded (included), depending on mode. To specify the Base IP, place a "0" in each byte of the address which is NOT common to all packets. For example, if you want *RouterScreen* to block traffic for IP addresses 192.168.193.1 through 192.168.193.254, enter "**192.168.193.0**" for the Base IP. Then use the Range feature to block that range of addresses (enter "**1**" for Low and "**254**" for High).
- **Multiplexing Byte** — Tells *RouterScreen* exactly which byte to multiplex the Base IP on (**A** for first, **B** for second, **C** for third, **D** for fourth) — wherever the first 0 appears. In the example above (see **Base IP**), the Multiplexing Byte would be **D**.
- **Range** — Tells *RouterScreen* the **Low** and **High** of the range of IP addresses that should be discarded/forwarded (see **Base IP**).

Optional (*depends upon individual network configuration*):

- **Single IP** — A single IP address that will be excepted from the rule set up by the filtering mode. Typically, this is the address of the router itself.
- **Multicast** — Allows multicast traffic to pass when **Yes** is selected (default is **No**).

- **Broadcast** — Allows broadcast traffic to pass when **Yes** is selected (default is **No**). If Yes, enter the subnet mask for the LAN/WAN nodes in the text box labeled “Broadcast Mask” within the appropriate port window in *iView*.

ABOUT BANDWIDTH CONTROL

RouterScreen has the ability to forward data in each direction (LAN to WAN and WAN to LAN) at up to 10 Mbps. You can set either or both directions to pass less than that (i.e., bandwidth control).

The bandwidth speed may be set independently for each port. As the actual Ethernet bit rate is always 10 Mbps, the bandwidth speed limitation for each port operates by extending the time between Ethernet packets so that the aggregate data rate matches the bandwidth setting. The algorithm used is intelligent enough to adjust “on-the-fly” to the length of each packet, resulting in a high degree of precision (within 5%).

Two parameters are used to specify the bandwidth: a **Bandwidth Granularity** common to both data ports, and an individual **BPS multiplier** for each port. The Bandwidth Granularity is typically used to establish basic units as power-of-2 or power-of-10 multiples (e.g., n x 1024 vs. n x 1000). You can allocate a specific amount of bandwidth to each port by enabling the Bandwidth Control function and entering a value for one or both ports.

NOTE

The value entered for a port is the maximum amount of bandwidth that the OPPOSITE port will output at any given time (i.e., LAN sets WAN, WAN sets LAN). Set bandwidth based on the FIRST *RouterScreen* port that traffic will come in contact with.

As stated, bandwidth control is calculated by multiplying the specified Bandwidth Granularity by the specified BPS. **If the total equals 0, it means that Bandwidth management is NOT enabled on that port.** The default Granularity is 1, and the default BPS for each data port is 0 (**1 x 0 = 0, NOT enabled**).

If you want speeds similar to 2B ISDN speeds, set the Granularity to 1000, then set the BPS for the port to 128. This provides 128K of bandwidth for the port (**1000 x 128 = 128K**).

You can give each data port a specific amount of Mbps by setting the Granularity to 1,000,000. Then, set the BPS for a port to 1 if you want 1 Mbps, 2 if you want 2 Mbps, etc. (**1,000,000 x 2 = 2 Mbps**).

To allocate bandwidth using *iView*, enter the desired Bandwidth Granularity in the Unit Configuration Window (choose Unit tab) and click **Set**. Then, for each data port, click the appropriate port tab (LAN or WAN) and enter the desired BPS value in the text box labeled “New” (lower-right of screen). Click **Set** to save settings.

LED Operations

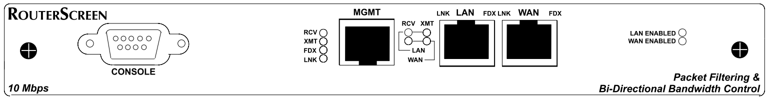


Figure 4: *RouterScreen Faceplate*

RouterScreen features status LEDs for each port (as shown above). The LED functions are:

RCV	Blinks yellow when port is receiving data.
XMT	Blinks green when port is transmitting data.
FDX	Glows yellow when Full-Duplex mode is selected on port.
LNK	Glows green when a link is established.
LAN ENABLED	Glows green when LAN port is enabled.
WAN ENABLED	Glows green when WAN port is enabled.

Other Applications for RouterScreen

RouterScreen may be used for many other applications in addition to router performance enhancement. Following is one example.

LIMITED BANDWIDTH SIMULATION

You can use *RouterScreen* to determine how Web sites (or other applications) will appear to users with a low-speed connection. Put *RouterScreen* between the LAN and a PC, set it to forward all traffic (All Protocols mode) and use the bandwidth control function to simulate line speeds from 14.4 Kbps dial-up to 1.5 Mbps T1.

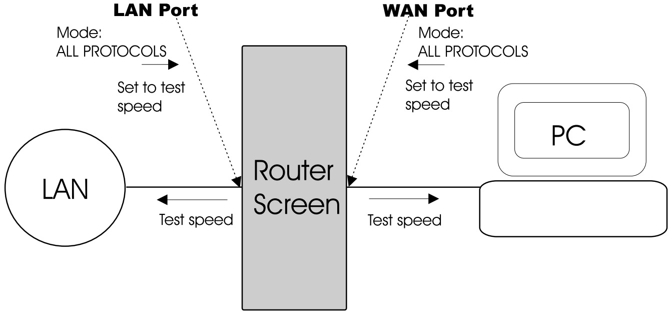


Figure 5: *Limited Bandwidth Installation*

Troubleshooting

- If there seems to be no communication between the ports, set the packet filtering modes for both ports to **All Protocols**, eliminate any bandwidth control settings, and check again. Then re-set the individual packet filtering settings for the ports.
- Sometimes, depending on the speed of the management PC and/or its video card, the bandwidth displays in the LAN and WAN port windows in *iView for RouterScreen* may not update when switching between windows quickly. To update the display, click the **Refresh** button found in the upper-right corner of the window.
- The *iView for RouterScreen* online help file requires Internet Explorer™ 4.0 service pack 2 or higher.

Should you encounter further difficulties, please contact IMC Networks technical support.

General Information

IMC NETWORKS TECHNICAL SUPPORT

Phone:	(949) 465-3000 or (800) 624-1070 (in the U.S.); +32-16-550880 (Europe)
Fax:	(949) 465-3020
E-Mail:	techsupport@imcnetworks.com
Web:	www.imcnetworks.com

SPECIFICATIONS

Environmental

Operating Temperature: 32° - 104° F (0° - 40° C)

Storage Temperature: 21° - 160° F (-6° - 71° C)

Humidity: 5 - 95% (non-condensing)

Dimensions (standalone unit):

2”H x 12”L x 7.02”D (5.08cm H x 30.48cm L x 17.83cm D)

3.9 lbs. (1.8 kg)

Electrical

Standalone/Chassis: 100/240 VAC ±10%; 0.1/0.05 Amp. (typical)

Module: 5V ±5%, .5 Amp. (typical)

ELECTROSTATIC DISCHARGE PRECAUTIONS

Electrostatic discharge (ESD) can cause damage to your add-in modules. Always observe the following precautions when installing or handling an add-in module or any board assembly:

1) Do not remove unit from its protective packaging until you’re ready to install it.
2) Wear an ESD wrist grounding strap before handling any module or component. If you do not have a wrist strap, maintain grounded contact with the system unit throughout any procedure requiring ESD protection.

WARNING! Integrated circuits and fiber optic components are extremely susceptible to electrostatic discharge damage. Do not handle these components directly unless you are a qualified service technician and use tools and techniques that conform to accepted industry practices.

3) Hold boards by the edges only; do not touch the electronic components or gold connectors.
4) After removal, always place the boards on a grounded, static-free surface, ESD pad or in a proper ESD bag. Do not slide the board over any surface.

WARRANTY

IMC Networks warrants to the original end-user purchaser that this product, EXCLUSIVE OF SOFTWARE, shall be free from defects in materials and workmanship under normal and proper use in accordance with IMC Networks' instructions and directions for a period of six (6) years after the original date of purchase. This warranty is subject to the limitations set forth below.

At its option, IMC Networks will repair or replace at no charge the product which proves to be defective within such warranty period. This limited warranty shall not apply if the IMC Networks product has been damaged by unreasonable use, accident, negligence, service or modification by anyone other than an authorized IMC Networks Service Technician or by any other causes unrelated to defective materials or workmanship. Any replaced or repaired products or parts carry a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

To receive in-warranty service, the defective product must be received at IMC Networks no later than the end of the warranty period. The product must be accompanied by proof of purchase, satisfactory to IMC Networks, denoting product serial number and purchase date, a written description of the defect and a Return Merchandise Authorization (RMA) number issued by IMC Networks. No products will be accepted by IMC Networks which do not have an RMA number. For an RMA number, contact IMC Networks at PHONE: (800) 624-1070 (in the U.S.) or (949) 465-3000 or FAX: (949) 465-3020. The end-user shall return the defective product to IMC Networks, freight, customs and handling charges prepaid. End-user agrees to accept all liability for loss of or damages to the returned product during shipment. IMC Networks shall repair or replace the returned product, at its option, and return the repaired or new product to the end-user, freight prepaid, via method to be determined by IMC Networks.

IMC Networks shall not be liable for any costs of procurement of substitute goods, loss of profits, or any incidental, consequential, and/or special damages of any kind resulting from a breach of any applicable express or implied warranty, breach of any obligation arising from breach of warranty, or otherwise with respect to the manufacture and sale of any IMC Networks product, whether or not IMC Networks has been advised of the possibility of such loss or damage.

EXCEPT FOR THE EXPRESS WARRANTY SET FORTH ABOVE, IMC NETWORKS MAKES NO OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THIS IMC NETWORKS PRODUCT, INCLUDING WITHOUT LIMITATION ANY SOFTWARE ASSOCIATED OR INCLUDED. IMC NETWORKS SHALL DISREGARD AND NOT BE BOUND BY ANY REPRESENTATIONS OR WARRANTIES MADE BY ANY OTHER PERSON, INCLUDING EMPLOYEES, DISTRIBUTORS, RESELLERS OR DEALERS OF IMC NETWORKS, WHICH ARE INCONSISTENT WITH THE WARRANTY SET FORTH ABOVE. ALL IMPLIED WARRANTIES INCLUDING THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY LIMITED TO THE DURATION OF THE EXPRESS WARRANTY STATED ABOVE.

Every reasonable effort has been made to ensure that IMC Networks product manuals and promotional materials accurately describe IMC Networks product specifications and capabilities at the time of publication. However, because of ongoing improvements and updating of IMC Networks products, IMC Networks cannot guarantee the accuracy of printed materials after the date of publication and disclaims liability for changes, errors or omissions.

Federal Communications Commission Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A computing device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

The use of non-shielded I/O cables may not guarantee compliance with FCC RFI limits.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le ministère des Communications du Canada.

Safety Certifications (standalone unit)

UL: Listed to UL1950 and CSA 22.2, No. 950, Safety of Information Technology Equipment, Including Electrical Business Equipment.

CE: The products described herein comply with the Council Directive on Electromagnetic Compatibility (89/336/EEC) and the Council Directive on Electrical Equipment Designed for use within Certain Voltage Limits (73/23/EEC). Certified to EN 60950, Safety of Information Technology Equipment, Including Electrical Business Equipment. For further details, contact IMC Networks.

LISTED 5M80
ITE
E156766